Electronic land register which forcefully eliminates real estate fraud and corruption

IPRA-CINDER

XIX World Registry Law Congress

Santiago de Chile 2014

The authors:

Ingmar Vali

Kadri Laud

Loori Paadik

Tallinn 2014

Introduction

We live at the end of the paper era. The times when people run with a pile of papers from one state agency to another are over. The age of technology has been replaced by the age of internet, and the land register customers are online wireless and in real time. It is time to let go of old dogmas and create services needed by the society. The digital revolution in state services happens just as fast as the increase in the number of smart phones owned by citizens. Are there any risks brought about by the digital revolution? Of course, but they do not compare to the risks of the paper era system. This article analyses the risks and problems before and after the development of electronic services. Furthermore, it highlights best-practices based on the Estonian example.

Estonia, reborn at the same time with the Internet, has now become one with it. In a country, where the President communicates with people through Twitter and Facebook and the Internet is a human right, people cannot even imagine that one would need a paper certificate in the land register to carry out a real estate transaction. The land register is available online and, in order to prove one's ownership, all one needs to do is to perform a query on their mobile phone. Instead of preventing the ink from fading on paper and protecting the papers from flood, Estonian registrars are currently eliminating the weaknesses that appeared in the first Estonian cyber-war and are restructuring legacy systems. Despite that this might seem as science fiction to some, it is, in fact, reality in Estonia. The experience gained transforming paper register into electronic is worth sharing. It is good tradition and good practice in Estonia to learn from the best or from the biggest mistakes, so that it is possible to avoid them.

Electronic registration in Estonia

The entire process of registration- conveyancing of immovable property is electronic in Estonia. This means that the preparation, forwarding and processing of registration applications and the making of registration entries takes place in an electronic environment. Almost 70% of all registration applications are submitted through a notary. The law stipulates that most of real estate transactions shall be notarised. This means that a notary prepares the documents for a transaction and the parties of the transactionsign it at the presence of the notary. After the transaction is signed, the notary submits the documents of the transaction

and a registration application to a land registry department to be registered and processed. The exchange of information between a notary and a land registry takes place electronically.

A notary prepares documents of a transaction on the E-Notary information system, i.e. the documents are electronic already when they are being prepared. After signing a transaction, a notary forwards the documents and a registration application through a safe data exchange layer, X-Road, to the land register information system, where it is automatically registered. The order of receipt of a registration application is important, which is why a notation on all received applications is available to the public online. Registrars working at the land register of a court commence the processing of a registration application when the turn of that application comes. As said above, the entire process is electronic. This means that additional data from paper is not entered in the system, because that data has already been entered by a notary, and an entry made as a result of the proceeding is also prepared in the information system of the land register. Decisions or entries made are available on the public [web interface](#) of the land register immediately after being signed by a registrar. After signing an entry on the information system of the land register, employees of the land registry department send parties to the transaction a notice on the making of a decision by email. Parties will be able to access the decision online and the system registers whether they have received the order.

All other applications not submitted through a notary are submitted through the [Immovables Portal.](#) The Immovables Portal is a public web portal developed especially for the submission of applications to the land register. Anyone who wishes to submit an application to the land register may use the Portal. The law stipulates which applications should be submitted through a notary and which ones can be submitted via the Portal, depending on the content of an application. The Immovables Portal is most commonly used by citizens, bankers, bailiffs, trustees in bankruptcy, state agencies, employees of local governments, etc. Similarly to applications received through the E-Notary, applications received through the Immovables Portal are registered automatically in the information system of the land register. After registration, a registrar commences the proceeding of an application and the rest of the proceeding continues just like in the case of documents received from the E-Notary described above.

Therefore, anyone who would like to submit an application to the land register, cando it through the Immovables Portal or at a notary. As of 2011, land registry departments do not accept applications submitted on paper or by email.

Estonia's transfer to electronic land register

After regaining its independence, the Republic of Estonia saw the establishment of land register in 01.12.1993. At first, the register was maintained on paper. In the last years of the previous century, it was decided that the land register should be electronic, and in 2000, the first version of the information system of the land register was completed. Unfortunately, the first information system of the land register was not successful. In addition, it appeared that the system lost data. Looking in the future, it was clear that continuing on paper was not a solution. It was decided to learn from the mistakes made and take another shot with the development of an information system. In 2006, a new version of the information system of the land register was introduced. One of the first tasks in the new information system was to check the integrity of data in the register. This meant that the electronic versions of the registry cards of all immovable properties were to be compared manually to the versions on paper and confirmed by electronic signature. This was a very time-consuming, but an extremely relevant task. As a result of the check, it was possible to declare that the developed electronic register was 100% accurate and, as such, has a legal meaning. From this point on, all entries made were done electronically and paper was sent to be archived.

In the first years of using the new information system, applications and other documents were submitted to the land register on paper, and employees of the land registry department registered the applications submitted and the relevant META data manually in the information system. After registration, the documents were enclosed to the paper file of the immovable which was maintained in the archive. The volume of the archive increased to the size where it had to be decided whether to build new facilities for the archive or to invest in the digitising process. However, the registration proceedings conducted by the registrars were already being carried out in the introduced information system. Moreover, all the entries made as a result of proceedings were maintained electronically. Everyone was able to access the entries made in the land register through a public web interface.

In 2007, notaries started using the E-Notary information system. The E-Notary was attached to the information system of the land register and from then on all notaries submit documents to the land register electronically by using the data exchange layer X-Road. The authenticity of documents was guaranteed by digital signature. Thus, about 70% of applications and

documents were submitted electronically. The rest of the applications and documents were still submitted to the land registry department on paper, which meant that more documents were added to the paper files.

In 2009, a change was made in the work process and the information system as a result of which land registry departments refused to accept registration applications and other documents on paper. All documents submitted on paper were immediately scanned and maintained in the digital archive. The original was returned to the applicant. Also, registration applications and documents enclosed thereto could also be submitted by email, while being equipped with an electronic signature. Thus, as of 2009, no new documents are added to the paper archive of the land register and all the new documents added in a land registry file are kept in the digital archive. However, all the documents submitted beforehand were still on paper, which made it more difficult for registrars to conduct proceedings as some of the necessary documents were digital and some had to be looked for in paper archives. Also for the citizens access to the land registry file documents was inconvenient.

As mentioned above, land registry departments accepted registration applications by email. However, as email was not a safe-enough channel for the submission of conveyancing documents, in 2011 the Immovables Portal, which was created especially for submission of applications to the land register was introduced. The Immovables Portal is used by anyyone, except notaries, who wishes to submit an application to the land register. Thus, as of 2011, all documents are received in the land register digitally through the E-Notary or the Registered Immovables Portal. As of the introduction of the Registered Immovables Portal, the land registry departments need not digitise applications on paper, as paper applications are no longer accepted. The same applies to the applications sent by emaile.

In 2010, a project with the aim to scan and digitally stamp all documents of land registry files contained in the paper archive was initiated. Digital stamping is important, because it closes the amendment of a scanned document. At the beginning of the project, there were about 800,000 paper files and each file had, on an average, 50 pages. Thus, about 40,000,000 pages were digitised in the project. The project of digitising documents has been extremely successful, and by the end of 2014, the entire paper archive of the land register will be digitised. All paper files of the land register will be transferred to and stored by the Estonian National Archives. In addition to the fact that for the registrars, the proceedings will be much

more convenient to conduct, a digital archive will enable to better plan the division of tasks and workload. Previously, proceedings had to be conducted at the location of the paper archive, but now, registrars can conduct proceedings on all applications regardless of where they are physically located, as all the necessary documents will be available online at all times. The information system has made the work of registrars aloteasier.

Risks and problems in introducing a software system

As mentioned above, the electronic land register makes the conducting of registration proceedings much more convenient. For example, compared to typing in entries, where each entry had to be printed on paper manually by a registrar, the information system enables to prepare and sign hundreds of entries at once. Moreover, since the system has decision templates, registrars no longer have to enter full texts of entries. The information system adds the META data determined by a registrar to the template and generates entries. In addition to convenience, simplicity and speed, the use of the information system is safer because it is next to impossible to generate fake land title certificates as all the information can be verified electronically in real time. However, the use of information technology does involve some risks.

The introduction of the new system involves various risks and problems. Below, we have listed some of the most important ones:

The stability and availability of the new system in the working environment. In order to keep the system reliable and usable, it is important to keep the system stable in the working environment, which means that the non-function time of the system has to be brought to a minimum. This is important because there is no alternative to verify the ownership from as the electronic data has legal value.

The compatibility of the new system for the performance of the intended tasks. One of the risks is the incompatibility of the system for the performance of the intended tasks, which would mean that the new system is not what is expected. The purpose of each new system should be to expedite processes and make them more effective, convenient and safe. Therefore, the new system should provide additional value compared to the previous situation. If, at the time of development of the system, the requirements of the processes and

the needs of the users were not explained in enough detail, it may appear in the introduction stage that the system is unsuitable for the tasks at hand. Even though the aforementioned risk only occurs very seldom, the situation, where the system is generally up to expectation but the requirements and needs of a few processes have not been realised to the maximum, is quite common.

Errors in the information system. In addition to obscure system requirements, errors also cause problems. An error in a software product may bring about the interruption of processes and extensive economic and reputational damage to a company or a public sector agency, because the intended functionality of processes is interrupted, which affects the earning of profit and the provision of a high-quality, fast and reliable service. Even if the system has been well-tested in the test period, it provides no guarantee that there are no errors in the system. The efficiency of testing determines the number of errors discovered, but one can never be sure that all errors have been discovered. Upon planning a software development project, it should be taken into account that in the implementation phase and afterwards there may appear errors which should be eliminated immediately. An organization that is supporting the register and software development process has to be introduced. For example, in the past, if a writing machine broke, the delay was minor because the error only interrupted the work of one registrar. However, if there is an error in the information system, the work of all users may be interrupted.

Maintenance stage. It is often forgotten that after introduction of a new system, i.e. the introduction of a software product, the maintenance stage follows, which basically lasts until the software is used. As a result of changes in the business environment, legislation or business processes, there may appear a need to modernise the software product. Also, the errors discovered in a software product in the introduction stage need fixing. For that, organization, resources and qualified work force should be planned to support the change.

The stability and compatibility of the work of interlinking mechanisms. If the system being developed uses other databases to verify and use information, one of the risks is the interruptions in the work of systems in a situation, where the interlinking mechanisms are unavailable. For example, in Estonia, the correctness of personal data is checked from the population register and the correctness of companies' data is checked from the commercial register. In order to manage risks, interlinking should be carried out already in the development stage so that even if an interlinking mechanism fails, the land register system

still works. On the other hand, it should be determined to what extent the failure to access data affects the processes of the system and what are the alternative solutions to process information. For example, it may be necessary to enter the data manually in the information system in case automation fails.

Transfer of data from the previous legacy system. In the previously used system, there are usually data which are necessary in the future. One of the bottlenecks may be the migration of data from the old data structure into the new one. The risk of losing data may be quite considerable. It is advisable to create means of automatic transfer, which areactivated only once to transfer data from the old system into the new. If the amount of data is small and/or the development of the algorithm for automatic conversion is too complicated, it is possible to transfer data manually. In this case, it may be necessary to create reports for the extraction of data from the previous system and entry forms or something similar for entering the data manually in the system being implemented. If the electronic data is of informative nature, there is a smaller risk of error. However, if the electronic data has legal effect, the loss of data must be prevented. For example, data is no longer printed on paper, so the electronic registers contain original information, which enables to determine who is the owner of an immovable or which mortgage has been established on an immovable. Should there be an error in data, someone may lose their ownership or a bank may lose their mortgage. If this should happen, the state shall be liable.

Human risk. One must also not forget the human risk, which may appear especially in the initial introduction of software. At that time there may appear a strong resistance from users. Some of that risk may be decreased by training. Also, some daily procedures need to be thought through. Can the procedures used so far keep functioning now that the software is being used? The answer is often no. This may bring about confusion among the users and add resistance to using new software. So, in addition to technical training on how to use the software system, employees need to be taught to conduct proceedings in a new way which has been carefully considered. Generally, upon implementation of a software system, the reorganisation of processes may be necessary. This endeavour has two sides – the adaptation of processes, which represents the organisational position and acceptance and approval which represents the position of an individual.

Human risk also includes wrongful adjustment of data for the purposes of personal gain. Below, there are some of the most notorious cases which have affected the registrars of electronic land registers in Estonia.

Real cases – fraud in land register and cyber attacks against Government institutions

We will give you a few examples/cases from real life, where the reliability of the land register has been abused from outside or inside the system.

The Tiesenhausen case

One of the few and most notorious real estate frauds is the so-called Tiesenhausen case. After the end of the Soviet period, the illegally occupied real estate was being returned to its former owners or their legal successors. Brunhild-Dorothea Tiesenhausen, a successor of the noble family of Tiesenhausen, owned a house in a valuable area of the Old Town in Tallinn, the capital of Estonia. The value of the house was about 1 million euros.

On 29 November 1999, someone initialled TT and a woman who presented a passport of Brunhild-Dorothea Tiesenhausen to be identified, appeared at the office of notary SR. Later, it was established that the passport was forged. The fake Tiesenhausen had the notary prepare a power of attorney for the selling of the house to TT, who sold the house to MK, who had served time in prison for several serious crimes. MK, in turn, sold the house to a company PR, which was established only days before the sales transaction. The real Mrs. Tiesenhausen only found out about the events six months later. She contacted a lawyer, who filed an action to the court for reinstatement of her right of ownership. A complicated investigation process and trial began. All three of these people were convicted and the building was returned to its rightful owner in 2004. The notary did everything in his or her power to identify the person and to establish the actual intent of the person. This was obviously a high-level forgery, which was impossible for the notary to detect.

With the help of today's electronic information systems and databases, the risk of such cases reoccurring has been brought to a minimum. A notary checks personal data from the population register, which also displays a photo of the person and more data about the person, which enable the notary to ask additional questions, e.g. on education, children, parents,

previous places of residence, documents, etc., should he or she have any doubts about the identity of a person.

The electronic land register provides an opportunity to check the status of the land register immediately before the transaction, which means it may be established who is the current owner and if there are any new applications concerning the immovable. A notary shall transfer the contract, immediately after the signature of the transaction, from the E-Notary system, via the X-Road (secure government hub) to the information system of the land register. Immediately a notation to the application (seal) appears, which indicates that changes in the data of the immovable are about to be entered. That prevents a notary from notarising a new transaction without examining the content of an unresolved application. This prevents the so-called double sales of immovable properties and other transactions violating immovable property ownership.

Persons concerned receive a notice and get a chance to access the data of the land register after the entry to the land register has been made. The notary who has notarised the transaction also receives a notice, and in reality the amendment in the land register is double-checked in order to make sure that the conveyancing and entries applied for have been made and that they have been made correctly.

Data exchange in the state takes place through a safe data exchange layer X-Road, which enables, in real time, to check the correctness of data and facts. If data is requested through the X-Road, there is no need to request for additional proof, paper certificate or contract. The X-Road was launched in 2001. The data exchange layer X-Road is a technical and organisational environment, which enables secure Internet-based data exchange between the state's information systems.

Violations committed by registrars

Entries in the land register are made by independent registrars. Upon making entries, a registrar is bound by law. Within the twenty years, when we have had the land register in the Republic of Estonia after it regained its independence, there have only been three cases when violations or intentional breach of duties by registrars have been established. One of the registrars was convicted in a criminal proceeding and two of them were released from office due to breach of duties. These acts were committed 10-15 years ago at the time when the land register was maintained on paper. Data was entered manually and could easily be altered without any traces in the system. Registrars violated the principle of the order of conducting proceedings on submitted applications. They took registration applications (on paper), and processed the applications submitted later before the ones submitted earlier. This created an unfair situation to those who had submitted their applications earlier. At that time processing times were long and this kind of behaviour by registrars may have happened more.

With an information system, the aforementioned violations are prevented as applications are registered automatically upon arrival. As of 1 June 2007, notaries are obliged to submit all registration applications electronically through the notaries' information system. And as of 1 June 2011, digitally signed registration applications can be submitted through the Immovables Portal. The division of application is automatic and equal. Subsequent alterations

in the processing order will be traceable in the information system. Applications may be re-divided to another registrar only by the head of the land registry department or at his or her request. There is a rule that applications should be processed in the order of receiving them.

Cyber attacks

Estonia is one of the first cyber attacked countries. In 2007, several cyber attacks took place which were aimed at, *inter alia*, the Parliament, the President, ministries, larger banks, news channels and communication companies. The attacks started after the riots that broke out after the transfer of a Red Army war memorial called the Bronze Soldier to a new spot. The transfer of the monument caused a heated conflict between Estonia and Russia. The information system of the land register was also under attack but not a lot of damage was caused, as this was a simple DOS attack (*Denial of Service Attack*). Farsightedly, the architects of the land register had constructed the system so that the outside world performs queries from the land register in one part of the database, where data cannot be changed, while registrars make entries in another part. Thus, the attack only interrupted the outer system and registrars did not even notice the attack. Following these events, the security of information systems has become an even more important priority.

In order to ensure security, Estonia has implemented the Standard of State E-Solutions' Security Measures (ISKE). The goal of implementing ISKE is to ensure a sufficient security level for the data processed in IT systems. The necessary security level is achieved by implementing the standard organisational, infrastructural/physical and technical security measures. It is an information security standard that is developed for the Estonian public sector. According to Government Regulation No. 273 of 12 August 2004, ISKE is compulsory for state and local government organisations who handle databases/registers. The first version of the ISKE implementation manual was completed by October 2003. The preparation and development of ISKE is based on a German information security standard – IT Baseline Protection Manual (IT-Grundschutz in German) – which has been adapted to suit the Estonian context. A three-level baseline system means three different sets of security measures for three different security requirements have been developed (different databases and information systems may have different security levels).

The land register has the highest security class. This means that, as one of the main state registers, it ensures the correctness, integrity and availability (or security in a larger sense) of

data in the land register. The establishment of an ISKE security level does not make the system more secure, but it provides instructions on which measures to apply. This makes it easier for a registrar to handle security issues.

Most of these requirements are procedural or easily implementable if sufficient financial means are available, but there are also some 'tricky' ones that cannot be met so easily. As mentioned above, we have given up maintaining paper register. We keep electronic data and changes made to them safe and intact. Every operation with these data is logged and saved.
The basic means of ensuring the integrity of data is a digital signature, which enables the person who made the change to be identified, while protecting the data or document by not allowing them to be changed without violating validity confirmation. Pursuant to the provisions set forth in the Code of Civil Procedure, documents submitted electronically to a land registry department must be signed digitally by the sender or submitted in a similarly safe way which would enable the sender and the time of sending to be identified (e.g. submitting documents through other information systems integrated with the information system of the land register). As a registration application can be either authenticated by a notary and sent via e-Notary or signed digitally and sent via other information systems. All electronically submitted documents are saved in the information system of the electronic land register with their digital signatures and thus their integrity is ensured. At the beginning of 2015, due to the requirements of ISKE, digital signing, hash chaining and time stamping of entries shall be implemented in the land register, in order to ensure the integrity of data (unauthorised changing and destruction of data).

Based on the defined security level, audits are performed on the implementation of the system of security measures. Auditing covers the compliance of hardware to requirements, the correctness of defining security classes and security levels, the selection and implementation of security measures taken. The person responsible for the database must make sure that the auditor has obtained the certificate of Certified Information Systems Auditor (CISA) granted by the Information Systems Audit and Control Association or the certificate of the ISO 27001 lead auditor granted by the British Standards Institute or the certified auditor's certificate granted by the German Bundesamt für Sicherheit in der Informationstechnik based on the ISO 27001 IT Grundschutz.

Legacy information systems

The first use of the term legacy to describe computer systems probably occurred in the 1970s. By the 1980s it was commonly used to refer to existing computer systems to distinguish them from the design and implementation of new systems. Legacy was often heard during a conversion process, for example, when moving data from the legacy system to a new database.

In order to analyse the so-called legacy problem of information technology, there should be discussion about the development of a state of the art information system among the stakeholders. Today, Estonia has one of the most effective and secure information systems of the land register. Due to the experience obtained in the process of development thereof, the good practice of maintenance of an information system was created. This deals with matters like how to develop and maintain E-Government systems. This chapter reviews some of the most important examples of this good practice, the use of which helps prevent the risk of excessive outdating of an information system and to ensure that the likelihood of successfulness of the development of new systems is greater.

An example from Estonia – what to do when an information system that has been used for years is outdated? Something that happened to the first information system of the land register in Estonia. The information system, which was created to help with the management of proceedings on paper, not to replace it, became more difficult to use year after year, and gradually started to interfere with the work of the users. In order to help users, a maintenance team had to be created. Problems piled up, and users found themselves stuck – there is work to be done but it cannot be done because the information system refuses to let them. However, users were resourceful and found ways to avoid the legacy software and do the work manually.

This caused a situation, where the information on paper title certificate was no longer in conformity with the electronic data. The more these situations occurred, the more work the maintenance team had to do to establish and fix the discrepancies. The security of the information system, which is compiled of availability, integrity and confidentiality, was seriously damaged. In such situations, it is important to include the management and make

decisions which enable to restore the work process of users and enable to develop a new software solution in the long run.

As mentioned before, shortcomings in software create possibilities for those who wish to abuse the system for personal gain. If software enables a user to make mistakes and violate the rules of procedure, then it is likely that the risk will occur. It is not always in bad faith, but that is for the management or court to decide.

How to renew an outdated legacy system

In a situation where the development of information technology has been standing still for years, the owner of the system will find himself or herself in a situation, where he or she has to create a new system because the improvement of the old one is no longer possible in most situations. But where to begin?

The creation of the new system is much easier than is often thought. You have to know what you want, write it down and order it. This theory works, if certain preconditions have been fulfilled. In order to create a successful information system, you have to draw up a project and an organisation, the purpose of which is to describe the old situation (AS-IS) and to develop the vision of the new information system and processes (TO-BE).

At first, you need to create a project organisation, which ensures the project with the necessary resources and capacity. Regardless of the size of the project, pursuant to good practice, a project organisation has a management group and a working group. Upon launching the organisation, the rules of procedure and the spheres of responsibility are agreed upon. The management group should include representatives of interested parties, people who are able to participate in the making of decisions related to the project. It is important to include the representatives of all of the larger stakeholders. Communication plays a significant role in the management group. Thus, the representatives of smaller stakeholders may be included in the meetings of the management group, if the decisions concern their field of activity.

The management group approves the budget, schedule and people responsible. In addition to resources, it is a good practice to approve the vision and objectives of the project. The

approval of vision is followed by the finding of a persons to carry it out and monthly supervision for which the working group is responsible. A project manager is appointed, who shall report to the management group and coordinate the exchange of information between the working group and the management group.

The objective of the working group is to resolve technical issues arising from describing the technical solution by analysts. The working group is a team with a project manager, an analyst, an administrator of changes and specialists of all parties concerned. In addition to technical issues, the working group shall resolve matters concerning the optimisation of process and legal issues. Thus, legislators and lawyers, who prepare the respective motions to amend for the management team, have to be included. If the single purpose of the project is to convert the process on paper into an electronic version, the result will be mediocre, which is going to facilitate the registration process to some extent, but will not be economic or make the process faster. Thus, upon launching a technology, it is important to take maximum advantage of its possibilities and to optimise the processes as well. The experience of colleagues from other countries who have gone through with the change is definitely very useful, since it helps save time and the risk of failure is lesser. The use of technology makes the processes more simpl and in some cases fewer employees are needed who may be used for the performance of other duties. For example, after the launch of the information system in Estonia, about 50% of registrar secretaries were dismissed, because the system is automatic. The workers were redirected to the digitisation of paper archives and thus the trained specialists did not lose their jobs but were given new duties instead. In the long run, when the digitisation of archives is completed, it will be possible to save considerably on staff costs. Changes are always painful, but when they are thought through, they will be smooth and the resistance from users will be kept to a minimum. Attention must be paid to changes and all parties be informed on the objectives and the benefits brought about by the changes in the short or long run. Changes may be made in stages, step by step, in order to ensure better control over the effects thereof and to change the course as needed.

The role of the Change Manager is necessary in every large project. Customers, specialists and the management keep interacting on what should be done to achieve the objectives and which decisions need to be made to do that. Changes may be made in the structure of the organisation, habits and means of work. Often, it is necessary to amend the legislation but that depends on the state. The administrator of changes should be included at the beginning of the

project because then he or she will be up to date with everything that is going on and will be able to perform his or her duties.

After the vision in place and organization formed, it is a good practice to describe the system requirements, i.e. the drawing up of the development order, which enables developers to provide price proposals. The more detailed the development order, the more detailed (and often the cheaper) the proposal, as the developer has no need to add risk buffers. The development order may be as detailed as necessary, up to detailed TO-BE processes and screen forms of the information system. However, a development order usually describes processes and requirements that are expected by the working group and the customers for the new system. In such case, it is important that the developer has an accurate understanding of the system to be created as this ensures less misunderstandings, errors and disputes later on. A decent vision and development order drawn up by experts ensures a great result.

What does a great result depend on
A considerable part of the success of the project depends on the quality of objectives, the experience of the people carrying them out, and communication, i.e. the administration of changes. For example, in Estonia, experts of business processes, legislation and technology have proven extremely useful. We call them business analysts, they are skilled in the field of land registry for a long time, and "translate" the requirements of the client (often registrars, lawyers) in the language of technology, so that developers would be able to understand them. As business analysts have knowledge of both areas, they understand the actual needs of users and how to fulfil them with the means of technology or to optimise them by changing the process. The inclusion of business analysis in the work of the working group has ensured Estonia with great results.

Sharing of experience and reuse of technology
We have achieved great results by learning from the mistakes of others and using their best practices. There is always a possibility to include colleagues from other countries, who have gone through the same development process successfully. Even though laws differ in different countries and their history is filled with various nuances, land registers are not that different. Looking at land registers through the eyes of a business analyst, all registers seem quite similar. The land registers in all countries serve the same purpose, although, it is more successful in some countries than it is in others. The primary object to be protected is an

immovable and the connection thereof to its owner. From the technical point of view, it is the same in all countries, so the means applied to achieve the objectives are the same. The fact that some of the registers are connected to the cadastre and some are not or the fact that some register contracts while others other make entries on the title page has basically no technical significance. Today, the needs of land register customers are the same – people want to search immovable properties by address and by the name of the owner of an immovable. In order to make the searches possible, the respective processes creating these structured data in the electronic register need to be developed to subsequently enable these searches. Even though land registers today are slightly different, their technical solutions in the future will be quite similar. Based on this theory, it would make sense to reuse the best system in the region to develop the next information technological solution and to introduce it according to one's own needs by making little adjustments. This would enable to save a lot of time, effort and money, which would be spent on the establishment of the architectural framework. Sometimes, there are several best practices available, which enable to compile the best combination and to order the perfect solution based on the examples which would be suitable for several countries or regions. Even the reuse of the best practice (e.g. vision) saves a lot of time and money and provides the best results. Looking at the big picture, in the future, joint developments are a possibility, where the main components (security, core functionality, etc.) are the same and the custom functionalities in each country are added as small adjustments. This model would considerably decrease the price of development of an information system and improve reliability and the quality of data. Also, the sustainability would be better ensured, because further developments and additions can be created together. It should be pointed out that the development of information systems today is relatively easy, but Estonia has reached a point where one has no-one to learn from anymore and the only way forward is to experiment and thus the development is considerably more expensive.

New technologies to be used
Starting from the most primitive, it would make sense to use the following technologies all of which contribute to the improvement of the quality of data, speed of the registration process and security. Good practice from Estonia:

1. Publication of the data in the land register is a great way to improve the quality of data and security and to decrease corruption. In Estonia, for example, all data of the land register are public and may be used by all state agencies free of charge. Private

persons may access the data for a charge through an online service. After the data was published, the quality of data improved considerably, because registrars as well as customers were interested in how the content of the register looked to the public. If there was a mistake, then the owner could see that and requested for the data to be corrected. In addition, criminal schemes related to immovable properties decreased, because everyone could check who the real owner of an immovable was, which made the real estate market safer.

If the data is public, the channels and technologies used by the customers of the land register should be used. There are e-services to be used in computers and smart phones, which ensure high-quality results in real time.

Data may be published in stages by first making them available to civil servants who have the need and obligation to check the data of immovable properties. Later, the data may be made available to other users.

2. The connection of an immovable and GIS data of the cadastre. Each immovable should refer to the plot of land and the geographical location. No immovable should exist without a plot of land. Such connection also improves the safety of the real estate market, because if the ownership of an immovable is connected to the land by GIS coordinates, there is no possibility of immovable properties existing fully or partly on the same physical plot of land or on the same plot of land having several owners. In Estonia, there are two registers, the land register and the cadastre, but the data are connected by cross-references and processes.

e-kinnistusraamat
Registrite ja Infosüsteemide Keskus

KINNISTUSRAAMAT

User name:
Company: Registrite ja infosüsteemide keskus
Session expires in 58 minutes.

Commercial Register   Immovables portal

| Search | My inquires | Admin | Help | User Information | Documents allowed for viewing | Log out |

Search:

| Location: | Address | |
| | Cadastral code | |

| Immovable: | Name of the registered immovable | | Former registered immovable number | | Land registry division | .. |
| | | | Registered immovable number | | | |

| Person: | First Name | vello | Surname | vagun | Legal Person | |
| | Personal identification code/registry code | | Former Owner | ☐ | Entitled person | ☐ |

Search   Cancel

Print

Registered immovable number	Former registered immovable number	Validity mark	Digital file	Land registry division	Type of immovable	Name of the registered immovable	Cadastral code	Address	Apartment no	Owner
555902	5559	*	*	Harju	Kinnisasi	Suurevälja 47	72701:002:0980	Harju maakond, Saue vald, Vanamõisa küla, Suurevälja tee 47		Vello Vagun (sünniaeg 11.11.1967)

New Search

Copyright (c) Registrite ja Infosüsteemide Keskus | Versioon 1.0.2 | Kasutajatugi tööpäevadel 9:00-17:00 telefon +372 680 3160, email rik.info@just.ee

Euroopa Liit
Euroopa
Regionaalarengu Fond

Eesti tuleviku heaks

3. The process on paper should be replaced by an electronic optimised process. It is quite easy to draw the existing process on paper and then make it electronic, step by step. In order to expedite the process, the experience of other countries may be used. Starting from input and ending with output, the entire process should be made electronic. The objective could be to improve data quality, expedite the process and to decrease expenses. In order to achieve the end result, laws and regulations should probably be amended and the electronic land register should be declared to be legally binding. The latter means that the electronic information has legal effect. Thus, there is no need for extracting data from the register on paper. Instead, everyone who would like to see who the owner of an immovable is, has to check the electronic register. One of the benefits is that the need for customer service decreases by about 50%. Paper certificates still exist to some extent, but the need thereof decreases by at least 95%.

4. Cross-usage with state registers, e.g. the cadastre, the population register, the commercial register, the construction register, the address register. Each state register has its principal data (data source). The principal data of the land register is the data of an immovable and its ownership (sometimes the data of restrictions and mortgages). Concerning the principal data of another register, they should be verified and imported from the respective register. If a new owner of an immovable should be registered, the data should be imported or verified from the population register, or, in the case of a company, from the commercial register, instead of typing it in from a paper copy. This enables to improve the quality of data and prevent typing errors. As mentioned before. in Estonia,, the exchange of data carried out through the X-Road.. Since data exchange between state agencies is free of charge and mandatory, it is very convenient to import data to land register.

5. The entire input in the register should be made electronic. Notaries, real estate agencies or banks, etc. who send input to the register should be directed to electronic channels. For example, in Estonia, notaries were obliged to submit applications and contracts to the register in an electronic form. Other applications from citizens and officials were also directed to an online portal, through which it was possible to submit applications to the register. Here, one of the criteria for success is authorisation and authentication. Secure means of e-identity authentication should be used. In Estonia, every citizen and official has an e-identity in the form of an ID-card. Users can authorise themselves through PKI (Public Key Infrastructure). Companies through their representatives can also authorise themselves and submit digitally signed applications to the register. This results in the fact that almost 100% of applications are submitted electronically by a notary or through the Immovables Portal. The users are aided by the fact that the law no longer permits the submission of applications on paper if it is possible through electronic channels.

6. Data protection. In order to ensure the security of an electronic register, it should be made sure that only authorised users have access to the changing of land register data. The risk of changing of data by an unauthorised user or due to a random error in software should be diminished. The larger the number of register users in the back-office and the size of the maintenance team, the bigger the risk of unauthorised data change. In order to ensure only authorised access to the system and the data, the tools of authentication and authorisation should be applied. In Estonia, the PKI (Public Key

Infrastructure) third party authentication programme is being introduced, which lets only Smart Card users access the system. In order to prevent unauthorised and unnoticed changes of data, an electronic signature has been implemented, which cannot be forged (not in the next decade). In addition, to prevent unauthorised deletion of data, the cryptographic hash values and hash chaining and log server have been taken into use. All of this is regulated by the procedures of IT management and maintenance and strict access rules. For example, external users cannot access the back office system, but all users can access the data in the database that is intended to be viewed and not changed.

7. Good practice of maintenance of information technology. For the purposes of maintenance and development of an information system, rules mandatory for all system developers should be established, i.e. the good maintenance practice. This ensures the sustainable maintenance and development of the system and the long life of the system. However, each system has a lifetime, as the technology around us develops with exponential acceleration, and when a system is outdated, it is difficult and expensive to supplement and maintain. For example, in Estonia, we have established an age limit to an information system as a good practice, in order to prevent the piling up of legacy systems. The possibility of development of the so-called legacy systems is limited and several times more expensive than the development of a modern system. Thus, it makes sense to agree upon the lifetime of an information system and to assemble a new project organisation in good time, which starts to update the information system. The so-called legacy systems slow down the progress and, in the worst case scenario, cause additional security risks.

The development of an information system is a continuous process. Just like a real town is never completed, so is an information system never really ready. It can be used, but there are always ways to update or supplement it. Each system is as ready as the amount of time and money allocated for that purpose allows. If there would be more time and money, a system could be more developed and better.

Summary

At first, there were slabs of stone, then papyruses, then books on paper and now databases. Do we know how a land register will be maintained tomorrow? Probably in a cloud. Estonia is definitely a country, where citizens and officials together develop the new services of the future, be they in a cloud or in a database of the land register prepared as a joint effort. It does not matter how much we try, the maintenance of a land register in different countries does not vary much technologically. Registers have similar objectives and problems and we use similar methods. Some countries have made bolder developments to their land registers and others keep firmly to their traditions. The land registers of some countries have transparent and secure processes while others do not. Putting the small details aside, the objectives of land registers are the same in most countries – the protection of the ownership of an immovable from unauthorised appropriation. As the objectives are similar, so are the methods and technologies and processes. Also, the needs of citizens and customers must be similar. Just like in the past, a seal or an image of a landlord's ring was needed to be applied on the document, we now also have to securely ensure the integrity of the electronic documents. Thus, the registrars maintaining the land register shall ensure the security thereof. Just like the doors and locks need to be replaced as the technology moves forward, we have to keep the security of the land register up to date and implement new preventative measures. It is very tempting to close the land register with a titanium door that weighs several tons, but even the thickest door fails to protect us from humanly mistakes, corruption and internal attacks. The door should rather be made of glass, so that everyone could see what is behind the door. That ensures that no-one even needs to break in. The transparency of the data of the land register has only benefitted Estonia, and we surely recommend it to others. Interestingly, the first reaction of people who examine this ideology is negative, because "then everyone can see what real estate I have". As indicated in the article, the making public of the data of the land register helps improve the security and fight corruption. Maybe the new transparency is rejected as a result of shady dealings. Because it is a well-known fact that if the accountant of a company is afraid to take a vacation because then someone else will see what is going on in the books, then it is quite certain that the accountant has set some aside for him- or herself. By implementing the modern technology correctly, these security risks can be considerably diminished.

Of course, the implementation of the new technology comes with some risks. There are courageous pioneers, who establish risks and possibilities before others. There is a lot to learn from their mistakes and success stories. Let us share more of our experience.

The use of new technology is certainly not cheap. And it gets more expensive every day. The lifetime of every new information system is 10-15 years, after which the system needs extensive repairs or a new system needs to be introduced.

However, if you calculate the expenses of land register customers who have lost their immovable properties due to fraud and the amount of insurance paid by the parties of a transaction in order to decrease risks, the preventive measures to ensure secure information systems is a drop in the ocean. The new land register in Estonia that we need to develop in the following years will probably be twice as expensive as the total investment of the previous information system (EUR 1.3 M). If itwere possible, we would use a secure solution developed for another country, because, as mentioned above, the functions and objects are quite similar.

Estonia is a small country in Europe which is like an experimental training area where one can try out different theories, because the changes are made fast and the mistakes can also be corrected fast. About changes, it should be considered that the value of going from a paper system to an electronic one is not in the fact that it is then electronic. One has to set the right objectives. It is important to change the processes and use the possibilities of technology supporting the main objective of the land register to a maximum extent. For example, in every new land register, security measures, e.g. smart card authentication and electronic signature/seal, should be implemented. A new technology requires new security measures. Just like in the paper world there are seals and certificate security paper, in the electronic world there are cryptographic chains and electronic signatures to guarantee the legal certainty. According to Estonian best practice, electronic maintenance of land register is more secure, effective, user-friendly and convenient for all users. To prove that, Estonia has given up the maintenance of a paper register and for years, the data of the land register has been public, electronic and has had legal effect. The results include a safe real estate market, handy e-services, and only a couple of cases of real estate frauds and exploitative abuse.

Share your experience so that we can all learn from it.